HEALTH CARE QUALITY AND COST COUNCIL
REPORTING PLAN SECURITY AND CONFIDENTIALITY MEASURES

All data collection, analysis and manipulation for the Health Care Quality and Cost Council are currently handled through the Council's various vendors. As a result the Council has required each vendor to ensure that the security, confidentiality and integrity of data are protected as part of their contracts with the HCQCC. Therefore, as part of the initial reporting plan, the Council has incorporated the confidentiality, security, and data integrity measures of its vendors. Summaries of the various data security, confidentiality, and integrity measures are attached.

Confidentiality, Security and Data Encryption

Protected Health Information Security

Data and patient confidentiality are critical. With over 30 years in data management, MHIC has extensive experience working with confidentiality rules and guidelines. All proprietary databases maintained by the MHIC are governed by confidentiality agreements that include rules for access as defined by the owners of the data. This confidentiality is applied to all data structures and, more specifically, to protected health information. In addition to the encrypted fields that are collected, we have extensive security mechanisms in place and a demonstrated culture of confidentiality at our organization. All MHIC employees are required to sign a confidentiality agreement upon employment. Failure to adhere to the agreement results in automatic termination.

MHIC will not use data collected as part of this contract for any purpose other than stated in the contract without the express permission of the Council. MHIC takes full legal and ethical responsibility for the use, release, and disclosure of information. MHIC will provide immediate notification to the Commonwealth of Massachusetts in the event of any unauthorized release of protected information.

There are two subcontractors working with MHIC for the management of Massachusetts health care claims data: Masspro and the Massachusetts Health Data Consortium. As described below, Masspro will provide off-site co-location facilities for the complete NCDMS system. The Massachusetts Health Data Consortium will assist with communication throughout the life of the contract. While neither contractor roles require access to the data, the subcontracts contain language prohibiting their use of the data without the express permission of the Council.

Security – Physical

The building which houses the MHIC is protected by a security system that requires both a key to unlock the building and a keyed code to disarm the security system. The computer room door is locked at all times, has a numeric keypad, and has limited access. A smoke and fire alarm system is connected to the security system.

The MHIC uses a variety of strategies to protect databases. The primary strategies are:

1. The use of standby databases (mirrored, synchronized database on a second database server) to create a live backup that uses completely independent hardware.
2. Nightly logical database backups (full exports) which are done by piping the exports through a compression utility (gzip) to reduce the sizes of the files before they are stored to the high-performance local file system on the database server. MHIC then copies these backup files across a dedicated gigabit network to near-line storage. The near-line storage servers combine large amounts of hard drive storage with high-capacity tape drives. The most recent copies of all database server backups are copied to weekly tapes, which are moved to an off-site storage location.
3. Off-site co-location facilities for the entire NCDMS system are provided by Masspro.

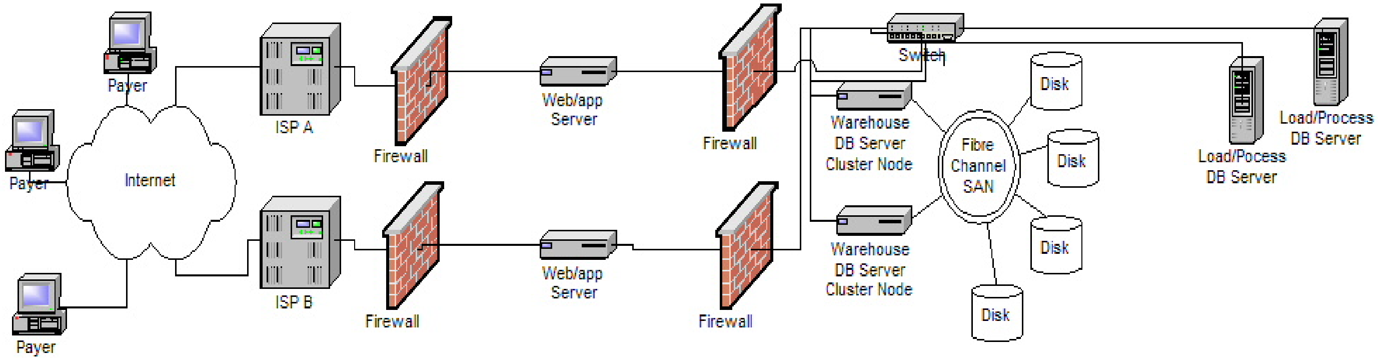
NCDMS
National Claims Data Management System

Confidentiality, Security and Data Encryption

MHIC

MHIC employs a multi-layer approach to security and at each layer every attempt is made to keep things simple and easy to monitor and maintain. The goal of this type of approach is to combine layers and components into an overall system that, when it fails, fails gracefully and safely. This approach can be partially compromised without failing completely, providing the administrator time to detect and respond to the problem.

Below is a visual example of NCDMS including our current data collection, processing and storage model.



Security and access to our systems starts at the reporter (payer) desktop using our encryption methodology.

Encryption

MHIC has developed a stand-alone one way data element encryption software that is run on the reporter's desktop before data is submitted to NCDMS. The encryption algorithm is a one way hashing algorithm using the industry standard SHA-512 protocol. SHA-512 is a computer security standard approved by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL). It is one of four secure hash algorithms described in the Federal Information Processing Standards (FIPS) Publication 180-2, Secure Hash Standard. The algorithms are distinguished by the length of the field to be encrypted. According to FIPS Publication 180-2 "The four SHA algorithms specified in this standard are called secure because, for a given algorithm, it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest. Any change to a message will, with a very high probability, result in a different message digest."

Confidentiality, Security and Data Encryption

In addition to encrypting the patient identifiers: Subscriber Social Security Number (ME008,MC007,PC007), Member's Social Security Number (ME010,MC008,PC008), Subscriber Last Name (ME901,MC901,PC901), Subscriber First Name (ME902,MC902,PC902), Subscriber Middle Initial (ME903,MC903,PC903), Member Last Name (ME904),MC904,PC904), Member First Name (ME905,MC905,PC905) and Member Middle Initial (ME906,MC906),PC906), this application performs preliminary verification of standard file formatting, verifies some header and trailer data elements, and produces a zipped text file ready for submission through secure web upload or by being written to CD or DVD and mailed.

Providing encryption software that is run by every reporter ensures that all patient identifiers are encrypted consistently across reporters and eliminates the possibility that direct patient identifiers are submitted. Since the encryption is done at the carrier's site, the carrier can easily verify that the personal health identifiers passed through the encryption software have been have been removed and replaced with an unrecognizable, encrypted 128 character field.

The external portion of NCDMS (www.ncdms.org) includes the secure web portal used by the reporter (payer) and by authorized users.

Security – External Network

Administrative access to the servers is limited to a secure shell (SSH). Telnet, FTP, and a number of other services which allow username/password information to travel un-encrypted across the network have been removed or disabled. Access from the Internet is controlled through a firewall by defining narrow sets of ports and protocols which are needed to support the Web server functionality.

MHIC uses a single purpose machine for its web server while other servers handle key tasks such as Firewall, VPN, File Serving, and Mail so that services/daemons not needed to function as Web Servers can be removed or disabled. Limiting the number of services running helps to limit the number of potential exploits on the server. MHIC installs regular patches and updates to security-related software (OpenSSL).

The internal NCDMS runs on an internal web server and consists of a series of Oracle stored procedures for editing, processing, managing and storing the data. This is broken into two components:

1. Redundant load/processing database servers in the upper right of the diagram which have the editing and processing stored procedures on them and
2. Clustered redundant warehouse DB servers that are connected to a fibre channel SAN which is the final location of the aggregated claims data.

Security - Internal Network

Internal administrative access to the servers is also limited to a secure shell (SSH) even for access from internal clients. General access to the servers is limited by account and specifically to the areas needed to maintain the web applications. Access to the external database is limited by both client address and username/password. Furthermore, system and database accounts are limited to those people who have a need to access the system.

Oracle 10g Enterprise Edition is the SQL relational database structure for the data warehouse and for all intensive data processing activity. Database structure resides on partitioned and clustered Enterprise Edition of Oracle 10g in a data warehouse attached by redundant fiber-channel switching to a RAID configured scalable storage area network (SAN). We also maintain an Oracle 10g Standard Edition of summarized data in the external DMZ of our network for the many applications that require report data available through web interfacing, this instance of Oracle is also integrated with our SAN.

This extensive security allows us to recover client data in a timely fashion and warehouse data within a twenty-four window.

Disaster recovery services housed at a Massachusetts facility and include the following:

- A cold backup of NCDMS that interacts with the payers and accepts data submissions (the web/app server). Masspro will provide ISP services and bandwidth to process data in the case of a failure at our primary facility.
- A cold backup of NCDMS that processes data submissions (the DB load/processing servers).
- A warm backup of NCDMS that provides long-term storage for processed data (the database warehouse). This is considered warm because we will be exporting daily transactions logs to the Council and keeping it up to date.

The disaster plan will be tested yearly at the Masspro facilities.

Additional security, access and release policies and procedures help to further protect confidential health information.

Secure Release and Audit

MHIC has standard procedures and policies in place that provide protection for secure receipt and/or release of information. In addition to our detailed security description provided we routinely provide the following functionality and compliance:

- Procedures that control access to secure information
- Security awareness and training for staff
- Logging and monitoring of access to data
- Procedures to respond to suspected or known security incidents.

These same procedures are applied in our handling of Massachusetts' dataset. In addition a logging mechanism will be used to accurately track the details associated with data release in conjunction with this contract. All MHIC response and reporting procedures will include designated Council staff where appropriate.

Data Access and Additional Requirements

The MHIC recognizes that the data belongs to the state of Massachusetts. MHIC may not use, release or grant access to any of the Council's data for any purposes other than those specifically authorized in the contract without the express written authorization of the Council. MHIC has a long, successful history of managing databases that are governed by similar restraints.

MHIC will comply with all state and federal laws in regards to Protected Health Information use and disclosure as will its subcontractors Masspro and the Massachusetts Health Data Consortium.